Italy’s Cybersecurity Architecture and Critical Infrastructure

ITALY'S CYBER SECURITY ARCHITECTURE AND CRITICAL INFRASTRUCTURE

Tommaso De Zan, Giampiero Giacomello, and Luigi Martino

Introduction

A long-standing member of the EU, NATO, OECD, and the group of G7 countries, Italy is by all measures a modern society with an advanced economy. Compared to other peers, however, such as France, Germany, Japan, or Canada, it is slower in adopting new technologies and integrating them into the economy. From the standpoint of cyber security, being a "sort of a latecomer" (Giacomello, 2005, 2018) allows the country to adopt policies and defenses already tested elsewhere. This lag, however, also means that Italy reacts to vulnerabilities slightly slower than other peers.

Italy's first computer network in 1980 was created by a group of nuclear physicists, with the intent of connecting all nuclear research institutes in the country (Siroli, Giacomelli, & Capiluppi, 1997) and it first connected to the internet (then ARPANET) on April 30, 1986, thus making Italy the *fourth* foreign country to do so (after the UK, Germany, and Norway). At the beginning, the internet was just one of several packet-switching networks that coexisted in Italy, while the dominant telecommunications firm at the time (SIP- Telecom) was trying to impose its privately owned system. Various cabinets at the time, aware of the importance of interconnectivity, supported integration among the networks. Ultimately, the adaptability and simplicity of the internet prevailed. Access to the internet was made available to private users after 1995, and the number of internet-service providers (ISPs) and users quickly soared. Since then, the Italian government has supported the internet as a catalyst for economic growth, increased tourism, reduced communication costs, and more efficient government operations. The most distinctive characteristic of Italy's information society, however, has been consumers' enthusiasm for mobile telephony and mobile internet, to the point that, already in 2009, Italy was in top position within the Organization for Economic Cooperation and Development (OECD) for mobile-phone penetration, with a rate of 151%.[1]

Broadly speaking, when it comes to cyber security Italy tries to stay within an "ideal" track represented by the EU on the one side and NATO on the other, incorporating directives and recommendations from both organizations, and trying to be a reliable partner (see, Dentons, 2018). This attitude is well illustrated, for example, by the events surrounding the visit of the Chinese president Xi Jinping in the spring of 2019. Worried

that by signing a memorandum of understanding with China for the "One Belt, One Road Initiative," Italy was opening its 5G infrastructures to the Chinese, when the EU and the United States expressed serious concerns, the government had to rush and adopt a presidential decree that guaranteed greater oversight on telecom infrastructures.

Unsurprisingly, today's concept of cyber security is larger than the purely technical dimension of IT-security, as it involves actors, malicious or protective, policies, and their societal consequences (Martino, 2018a). While Italian authorities have engaged, now and then, in issuing formal requests for the removal of some particular content, or for whole websites, by and large, the public has unlimited access to the internet and social media. In fact, today, a most worrisome sign that cyber security should include policy for social media not only because of possible "perception management" activities (see Horowitz, 2018), but also for the increasing opposition of the public, expressed on the social media, to issues such as immigration.

The next three sections of this chapter examine (a) the current status of cyber security measures in Italy and (b) Italy's initiatives and commitment to international initiatives to foster security in cyberspace, and (c) the current status of public–private partnership in cyberspace.

Italy's cyber security governance and policy

Although an official registry for critical infrastructures (CI) is still missing in Italy, similar to other advanced societies, these sectors are considered part of the CI (Brunner & Suter, 2008: 211–212):

- Banking and finance
- Public safety and order
- Communications
- Emergency services
- Energy production, transportation, and distribution
- Public administration
- Health care systems
- Transportation (air, rail, maritime, roads) and logistics
- Water
- Information services and media
- Food supply

The CI along with the rest of cyberspace have recently become the focus of policy-makers and cabinets alike.

In Italy, cyber security governance and policy are outlined in two different documents, respectively the Quadro Strategico Nazionale (QSN), which defines the responsibilities and roles of the institutional actors involved in cyber security, and the Piano Nazionale (PN), which outlines national objectives and action plans to achieve them. Taken, together these two documents form the Italian cyber security strategy. In the context of regulatory developments in the European Union (EU) and internationally, the second Italian cyber security strategy was issued in 2017,[2] four years after the publication of the first strategy under the government of Mario Monti. The new strategy was formulated with the intent to streamline the institutional governance of cyber security and increase operational capacity in the wake of the entry into force of the Network and Information Security (NIS) Directive,

which was nationally adopted in June 2018. This section argues that, whereas one can see clear developments in the institutional framework governing cyber security, Italian cyber security policy has not significantly changed since its inception in 2013.

With the new QSN, the main stakeholders within the Italian cyber security governance remain the President of the Council of Ministers (the Prime Minister) and the Interministerial Committee for the Security of the Republic (Comitato interministeriale per la sicurezza della Repubblica, CISR).[3] In terms of specific duties, while the President adopts the QSN/PN and gathers the CISR in the case of a cyber security crisis, the CISR proposes changes to the QSN/PN, monitors their implementation, smoothens collaboration among the various institutional actors, establishes national cyber security objectives, and proposes regulatory measures to strengthen cyber security, preventive, and mitigation measures. In terms of strategic policy making, the main difference from the cyber security governance set in 2013 is the role of the Director-General of the Security Intelligence Department (Dipartimento Informazioni per la Sicurezza, DIS), who has now gained a more direct and prominent role in defining the general policy aimed at improving the security of systems and networks.

At a lower level of the decision-making institutional layout, the two main bodies are the Technical CISR (CISR Tecnico, CISR-T), and the Cyber Security Unit (Nucleo Sicurezza Cibernetico, NSC). Chaired by the DIS's Director General, the CISR-T supports the CISR and implements the measures foreseen in the PN. Formally placed under the Office of the Military Advisor of the Prime Minister,[4] the NSC is now located within the DIS,

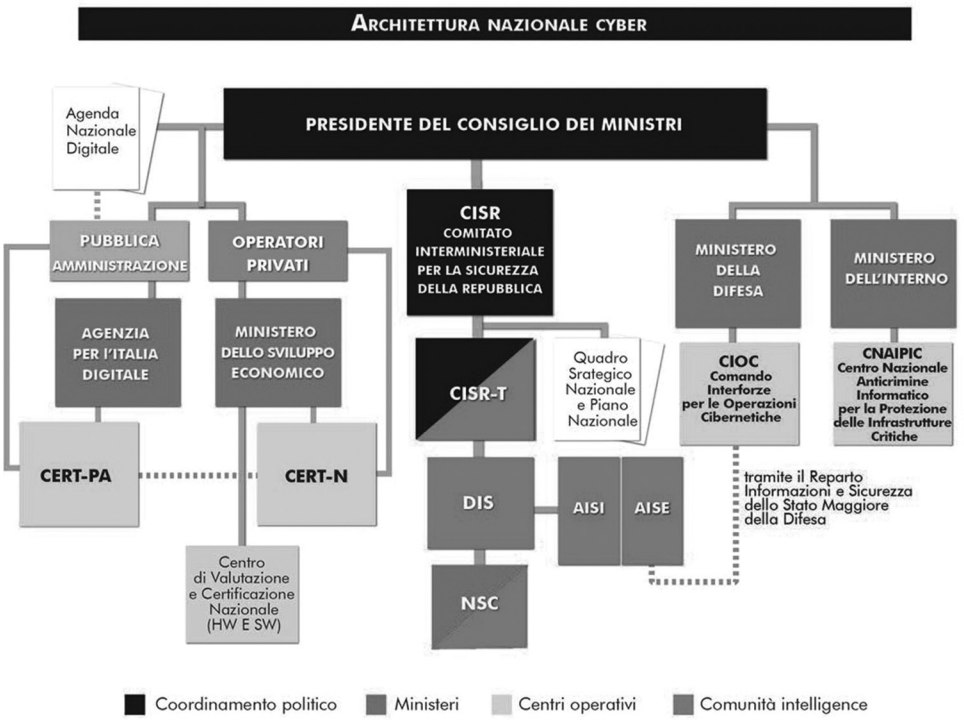

Figure 10.1 Italy's National Cyber Architecture

Source: Sistema di informazione per la sicurezza della Repubblica (2018).

and has the primary role to prevent and manage cyber crises, but also to promote cooperation among various ministries, coordinate information sharing activities, collect information regarding data breaches of ministries relevant to national security and, finally, be the main point of contact for international and regional organizations such as the EU, North Atlantic Treaty Organization, and United Nations. The NSC is chaired by the DIS's Deputy Director-General, who is the highest-ranking official of the Intelligence Department dealing almost exclusively with cyber security issues, including coordinating the various actors within the Italian cyber security governance and *de-facto* overseeing the implementation of the PN (Presidente del Consiglio dei Ministri, 2017).

The 2017 PN has the ultimate objective of developing the strategic objectives delineated in the QSN and, to achieve them, foresees 11 operational guidelines, which are the same guidelines of the 2013 PN. These are:

- strengthen intelligence, law enforcement, civil and military defense capability;
- strengthen coordination and interaction among private and public sector stakeholders;
- promote security culture, including education and training;
- international cooperation and exercises;
- increase operational power of national institutions dedicated to incident prevention, response, and remediation;
- international regulatory and compliance measures;
- compliance and security controls;
- support industrial and technological development;
- strategic communications;
- resources;
- implement a national cyber risk management system.

Compared to its predecessor, the new PN includes a separate Action Plan listing some priorities to ensure a rapid step change in the protection of the national cyber space in the years to come. After presenting the logic behind the establishment of the Joint Cybernetic Operations Command (Comando Interforze Operazioni Cibernetiche, CIOC), which is intended to achieve full operational capability by 2019 (Vestito, 2018), the Action Plan put forwards five new initiatives:

1 Merger of the CERT nazionale Italia and the CERT-Pubblica Amministrazione (CERT-PA) into a single operational structure called CERT-Italia;
2 Establishment of a national evaluation and certification center to verify ICT components embedded in strategic and critical infrastructures;
3 Creation of a foundation or venture capital fund to invest in innovative start-ups or relevant enterprises;
4 Establishment of a national research and development cyber security center in malware analysis, security governance, critical infrastructure protection, and threat analysis;
5 Creation of a national cryptography center involved in establishment of cyphers, development of a national algorithm and blockchain as well as security evaluations.

The NIS Directive came into force in Italian law in the form of legislative decree n.65 in June 2018 and spurred some relevant changes within the Italian cyber security institutional ecosystem. The DIS consolidated its position as the central Italian institution for cyber security policy, becoming the national contact point concerning information and systems

security matters. As a national contact point, the DIS is the national representative to the EU Cooperation Group, formed by EU Member States, the Commission, and the European Union Network and Information Security Agency (ENISA), with the role to ensure strategic cooperation and the exchange of information among member states in cyber security.

The Decree also designated the competent authorities with the important role of monitoring the national application of the NIS Directives: 1) Ministry of Economic Development (Ministero dello Sviluppo Economico) for the energy and digital sectors (both services and infrastructures); 2) Ministry of Infrastructures and Transport (Ministero delle Infrastrutture e Trasporti) for the transport sector; 3) Ministry of Economy and Finance (Ministero dell'Economia e delle Finanze) for the banking and financial market infrastructures; 4) Ministry of Health (Ministero della Salute) for the health sector; 5) Ministry for Environment, Land and Sea Protection (Ministero dell'Ambiente e della Tutela del Territorio e del Mare) for drinking water supply and distribution. To smoothen national cooperation, the legislative decree makes all these be part of the Joint Technical Committee (Comitato tecnico di raccordo), within the Presidency of the Council of Ministers.

In line with the new 2017 PN, the legislative decree also established the Italian CSIRT (CSIRT Italiano) which has the role of a unified computer and emergency response team, merging the functions of the two previous CERTs (CERT-PA and CERT-N). The Italian CSIRT is placed under the authority of the Presidency of the Council of Ministers with a team of 30 professionals and a budget of €700,000 from 2019 onwards (with an initial investment of €2,000,000).[5] The NIS Directive also included the Italian CSIRT in the EU CSIRT's network, which comprises of representatives of Member States' CSIRTs and the CERT-EU.

Analysis of the 2017 national cyber security strategy and policy

Looking at the evolution of Italian cyber security, one can argue that between 2013 and 2018, most of the changes have regarded the institutional framework rather than the formulation of cyber security policy.

In the first strategy, some experts had underlined how the structure of Italian cyber security governance could be improved and streamlined (De Zan, 2016a). In particular, experts viewed the old structure as fragmented and suggested to further centralize it and/or reduce the number of actors whose tasks were overlapping. Since 2013, DIS has consolidated its role as central cyber security actor thanks to its operational role in the security of systems and networks in the period 2013–2016 and the implementation of the NIS directive in 2018. The Intelligence Department is now the key actor within the Italian cyber security governance, similar to what happens in the United Kingdom, where the NCSC-GCHQ is the cornerstone of various aspects of British cyber security. Moreover, the new QSN has assigned to the DIS's Director General a newer significant role in the definition of priorities on cyber security matters, possibly filling a gap in terms of strategic leadership able to link the strategic with the operational level which was missing in the previous institutional layout. Furthermore, the new placement of the NSC under the DIS rather than the Office of the Military Advisor of the Prime Minister is also another factor that could let us conclude that with the changes occurred in the new governance, some of the institutional asymmetries that had been previously considered as problematic have been removed.

Apart from these changes to the Italian institutional arrangement, little seems to have varied in Italian cyber security policy since 2013. In addition to a renewed emphasis on the enhancement of CERTs, intelligence, law enforcement, civil and military defense capabilities, the 2017 PN presents five initiatives (those contained in the separate Action Plan, seen above) that are innovative with the respect to the previous plan. Nevertheless, the 11 operational guidelines of the newer 2017 NP are almost identical to those already formulated in 2013, actually worded almost in the exact same way. This could lead some observers to ask whether any significative advancement has been made in the period 2013–2017 and to what extent the objectives of the previous PN have been achieved. Already in 2016, analysts were questioning what type of evaluation mechanisms were in place to inform advancements in Italian cyber security policy (De Zan, 2016b). Despite several official documents having reiterated that a formal evaluation and analysis of lessons learned had been set up to inform the new QSN and PN (Sistema di informazione per la sicurezza della Repubblica, 2017, 2018), possibly for national security reasons, there is no public account of this evaluation process and whether the objectives of the 2013 strategy have been fully, partially or not met. Regardless of how rigorous this evaluation process was, one can argue that the striking similarities between the 2013 and 2017 PNs suggest that the course of Italian cyber security policy has not significantly changed since the first Italian cyber security strategy in 2013.

The Italian contribution to secure cyberspace

Italy recognizes an important role for diplomacy in cyberspace, in particular the activities conducted in multilateral and regional forums, such as the activities promoted by the United Nations General Assembly, the Organization for Security and Cooperation in Europe (OSCE), and the G7. Italian cyber diplomacy was consolidated both under the presidency of the G7 in 2017 and during the Italian Presidency of the OSCE in 2018. There, a priority of the presidency was to improve collaboration and cooperation between participating states in the cyber domain (Martino, 2018b).

In Italy, according to the National Cyber Security Strategy, international initiatives in the cyber domain must be divided into two macro-activities: operational and institutional. The operational activities are the responsibility of the Cyber Security Unit – *Nucleo di Sicurezza Cibernetica* (NSC) in Italian. In fact, according to the provisions of Art. 9, letter f) the NSC

> constitutes a national reference point for relations with the UN, NATO, the EU, other international organizations and other states, without prejudice to the specific competences of the Ministry of Economic Development, of the Ministry of Foreign Affairs and International Cooperation, of the Ministry of the Interior, of the Ministry of Defence and of other administrations foreseen by the current legisla- tion, ensuring any necessary connection in this matter.[6]

This activity is even more evident if we consider the legal framework produced by the NIS Directive which, at Member States level, establishes a national contact point in order to enhance the info-sharing mechanism at European Union level.

Meanwhile, the institutional and representative activities in international and regional forums are the responsibility of the Ministry of Foreign Affairs and Internal Cooperation (Ministero degli Affari Esteri e della Cooperazione Internazionale), which represents Italy in international forums and coordinates in close contact with the NCS.

Analysis of Italian cyber diplomacy

The Italian approach to cyber diplomacy relies firmly on international cooperation, favoring international and multilateral forums over bilateral ones. In particular, there are two initiatives that should be highlighted:

- The activities promoted by Italy in the OSCE, especially the active role in the implementation of Confidence Building Measures in cyberspace (OSCE Permanent Council, 2013, 2016).
- The proposals put forth during the Italian presidency of the G7 in 2017 – within the Ise-Shima Cyber Group of the G7 – regarding the declaration on the rules of responsible behavior of States in cyberspace, the so-called "Lucca Declaration," which highlighted, inter alia, the importance of applying existing international law in the cyber domain (Ministry of Foreign Affairs, 2017; Martino, 2018c).

In particular, the Italian international cooperation approach applied to the cyber diplomatic dimension is actively manifested both within the OSCE framework (OSCE, 2012),[7] whereas Italy, since 2012, has had a proactive approach within the Informal Working Group entirely dedicated to "cyber diplomacy," (c.d.) and within the G7 framework, where it is important to remember the work carried out under the Italian presidency of the IseShima Cyber Group.

As far as the G7 cyber activities are concerned, on the occasion of the Italian presidency of the ISCG, diplomatic initiatives were launched immediately to establish norms of responsible state behavior in cyberspace in alignment with the activities of UNGGE (Taormina Leader's Communiqué, 2017).

Although the negotiation process started from a proposal initially based on a "code of conduct" in cyberspace, with related appendices on verification and actions to be taken in case of attack and cyber incident, it evolved into a political declaration in the drafting phase. The declaration was then approved by the Ministers of Foreign Affairs as the *Declaration on Responsible States Behaviour in Cyberspace*, and finally endorsed in the *Leaders' Communiqué* of Taormina in May 2017. The "Lucca Declaration" recognizes the predominant role of states in the process of building a safer and more stable cyber environment; furthermore, it bases its legitimacy on the activities carried out by the UNGGE and the OSCE; finally, it recognizes the possibility of applying the existing international law to the cyber domain.

It is important to note that the work carried out by the ISCG, under the Italian presidency, has sought to intrinsically place the emphasis on the need to move from a predominantly technical approach (as it is currently the case at the UN where UNGGE has the power only to make recommendations and limits of "effectiveness" of this exercise are evident in the lack of consensus which caused the failure of the approval of the *report* 2017) to a purely political-diplomatic process that, ultimately, provides shared rules of conduct (with hope in the future also binding) valid for the specific case of cyberspace (Martino, 2018b).

The Italian public–private partnership approach in the context of cyber security

The existing national security policy framework refers to the public–private partnership as a more or less vague concept of protection of critical infrastructures from cyberattacks. In

fact, although the Italian National Cyber Security Strategy recognizes the PPP as an appropriate instrument to enhance the critical infrastructures protection (CIP) from cyberattacks, this policy statement is addressed by generic political or administrative instruments such as *Protocolli d'Intesa* (i.e., Memorandums of Understanding), which, in general, are not legally binding.[8]

Moreover, in Italy – according to publicly available data – any kind of written or clearly formulated legally binding PPP contract, in terms of accountability, responsibilities, risk allocation, obligations, duration or budget constraints which should underline roles and commitments between the governmental or state authorities and private CI-enterprises in the context of protection of critical infrastructures from cyberattacks does not exist. The lack of any formal contracts (or national laws) defining participants, responsibilities, and risks allocation marks a specific difference between the current Italian PPP policy approach on CIP-framework from the conventional or "classic" concept of PPP, which instead foresees a long-term partnership based on a legal binding framework (such as a contract), which defines obligations among the partners and allows risks allocation properly in order to achieve the outcomes.

Conclusion

As recently noted by Catalano, Graziano, and Bassoli (2015: 749), the fact that the national administrative model is "characterized by a high formalism based on the primacy of law, and the administrative process must rigorously be pursued within the limits laid down by abstract rules and legal precepts" has not really helped Italy's path to modernity. Operating in cyberspace and managing cyber security are at the opposite ends of such attitudes. Indeed, they are incompatible.

In cyberspace and, consequently, cyber security, Italy presents innovative niches along with backward areas, both in the private sector and in the public administration. Membership of the EU has proved to be a mixed blessing, as funds and expertise are available but come with regulations and peer pressure for the country to conform its cyber defenses and policies to those of its European partners (Fritzon, Ljungkvist, Boin, & Rhinard, 2007). The net outcome for Italy has been that of an "elusive information society" (Giacomello, 2018). The vulnerabilities of critical infrastructures will not go away and societies' dependence on them can only increase. That cyber security should become everybody's concern is inevitable, in Italy, as elsewhere in advanced societies. Hence, the training/sensibilization for users and businesses to cope with disruption and malfunctioning and to adopt responsible behavior in cyberspace should be a priority for any future Italian government, no matter their political inclination.

Overall, it is evident that Italy too has greatly benefited from the growth of cyberspace, the diffusion of mobile phones, and online banking. Nonetheless, in case of critical infrastructures failure and cascading disasters, it would be the government that would have to "foot the bill" after the society suffered the consequences. To avoid such outcome, the government and the private sector, via the PPP and other solutions, try to prevent such ominous situation. Yet, organizational theories show that the risk of failure is embedded precisely in such solutions. As Charles Perrow (2011 [1984]) prominently noted, institutional fragmentation, that is, too many stake-holders, negatively affect the ability to reliably manage critical systems and that the consequences could be quite dear. This conclusion certainly applied to the Italian case, but also to several other countries examined in this volume.

Notes

1 Organization for Economic Cooperation and Development (OECD), "OECD Key ITC Indicators – Mobile subscribers in total/per 100 inhabitants for OECD, 2007" available at: www.oecd.org/sti/ICTindicators.

2 The QSN was approved as a decree of the President of the Council of Ministers ("Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali") in February 2017. The related PN was made publicly available in March 2017.

3 The CISR is composed by: President of the Council of Ministers, Delegated Authority, Ministry of Foreign Affairs, Ministry of Interior, Ministry of Defence, Ministry of Justice, Ministry of Economy and Finance, and Ministry of Economic Development.

4 The NSC comprises all the ministries of the CISR-T in addition to representatives of the Italian intelligence services (AISE and AISI), Military Advisor (Consigliere Militare) of the President of the Council of Ministers, Department of Civil Protection, and the Agency for Digital Italy.

5 The total budget for the implementation of the NIS directive was €5,300,000 in 2018, and €3,300,000 from 2019 onwards (Art. 22).

6 See, www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html.

7 On April 26, 2012, the OSCE, with the decision of the Permanent Council n. 1039 (PC.DEC/1039), established the informal working group (IWG) aimed at developing CBMs to reduce the risk of conflicts in the cyber domain. The work of the IWG led to concrete results in 2013, when all 57 OSCE participating states, through the PC.DEC/1106, approved an initial set of 11 CBMs focusing mainly on transparency measures and communication channels and trust. In March 2016, the OSCE adopted additional CBMs contained in the Permanent Council decision n. 1202 (PC.DEC/1202). This second set focuses on measures based on cooperation between participating states in cyberspace, emphasizing, for example, the mitigation of cyberattacks against critical infrastructures and highlighting the risk of such attacks being able to have consequences, like a domino effect, on the entire organization. Finally, on December 9, 2016, the OSCE Ministerial Council, meeting in Hamburg, approved a specific decision on OSCE activities in cyberspace, marking the first document of this kind adopted by the highest political level of the Organization in the field of cyber security. It is useful to recall, for example, the direct involvement of Italy in the OSCE project "Enhancing the implementation of OSCE CBMs to reduce the risk of conflict stemming from the use of ICTs" carried out between 2016 and 2018 in collaboration with the University of Florence as an implementing partner and with other universities at an international level as project collaborators. The project, through a comparative analysis and a "cyber profiling" of the 57 participating states of the OSCE has allowed, among other things, to identify the obstacles that countries face in the application of Confidence Building Measures in cyberspace and to advance a Specific "Action Plan" for overcoming these obstacles through targeted capacity building programs.

8 As stated by the National Center for Counter Cyber Crime and Critical Infrastructures Protection (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, CNAIPIC), the national competent body to protect CI from cyberattacks: "The [CNAIPIC] operating model is based on the principle of 'public–private' partnerships: the CNAIPIC, in fact, assumes (through an operational room available 24/7) a central location within a network of critical infrastructural realities (institutional and business), and works in close connection with various organizations (national and international), engaged in the specific sector as well as on the issue of information security, with which it maintains constant relationships of information exchange and provides (through intelligence and analysis units) the collection and processing of data useful for the purpose of preventing and combating the threats. The aforementioned partnership relationship finds its moment of formalization in the stipulation of specific agreements [i.e., Protocolli d'Intesa]; since 2008, agreements have been stipulated, among others, with the following entities and companies: ENAV, Terna, Aci, Telecom, Vodafone, Ffss, Unicredit, Rai, Consob, Ansa, Atm – Milanese Transport Company, Abi, Banca D Italy, Sia Ssb, Intesa Sanpaolo, Enel, Finmeccanica, H3g, Atac, Expo 2015." See, Ministero dell'Interno, CNAIPIC "Comunicato Stampa," May 14, 2017, www. commissariatodips.it/uploads/media/comunicato.pdf; (Italian Original translated by Luigi Martino). As regards the Memorandum of Understanding see: Ministero dell'Interno, Accordo tra ministero del- l'Interno e Terna per la sicurezza della rete elettrica nazionale, July 30, 2009, www1.interno.gov.it/

mininterno/export/sites/default/it/sezioni/sala_stampa/notizie/ministero/0519_2009_07_30_accordo_con_Terna_per_sicurezza_rete_elettrica.html_1840113086.html; Polizia di Stato "Intesa con Vodafone per la sicurezza informatica," January 20, 2010, www.poliziadistato.it/articolo/17950-Comunicazioni_intesa_con_Vodafone_per_la_sicurezza_informatica; Confederazione del Commercio Regione Lombardia, "Protocollo d'Intesa Cyber Security tra Polizia Postale e delle Comunicazioni Lombardia e Confcommercio Lombardia," August 2, 2017, www.confcommerciomantova.it/uploads/articles/1664/Protocollo%20d%27Intesa%20Cyber%20Security%20tra%20Polizia%20Postale%20e%20delle%20Comunicazioni%20Lombardia%20e%20Confcommercio%20Lombardia.pdf; Aska News, "Cyber crime, intesa Polizia-Mps" Cyber-Affairs, March 13, 2018, www.askanews.it/cronaca/2018/03/13/cyber-crime-intesa-polizia-mps-per-contrasto-a-reati-informatici-pn_20180313_00073/; Agenzia Regionale per la protezione dell'ambiente ligure ARPAL, "Firmato digitalmente protocollo di intesa Arpal – Polizia postale e delle comunicazioni" April 28, 2018, www.arpal.gov.it/articoli/58-temi-news/3521-firmato-protocollo-di-intesa-arpal-polizia-postale-e-delle-comunicazioni.html; Polizia di Stato, "Accordo tra Terna e Polizia di Stato contro i crimini informatici," May 10, 2018, www.poliziadistato.it/articolo/135af4444513904707267764; Quotidiano Sanità, "Sicurezza informatica. Protocollo d'intesa tra l'Asp di Cosenza e la Polizia di Stato per contrasto a reati informatici," May 18, 2018, www.quotidianosanita.it/calabria/articolo.php?articolo_id=61921; (all documents consulted June 13, 2018). However, the specific aspects related to the Italian approach on CIP will be addressed in the section of this thesis entirely dedicated to the analysis of the Italian legal-political architecture in the context of critical infrastructure protection from cyberattacks, taking into account the legislative changes introduced by the aforementioned implementation of the European Directive "Network and Information Security."

References

Brunner, E. M. & Suter, M. (2008). *International CIIP Handbook 2008/2009*. ETH Zurich, Switzerland: Center for Security Studies.

Catalano, S., Graziano, P., & Bassoli, M. (2015). "Devolution and Local Cohesion Policy: Bureaucratic Obstacles to Policy Integration in Italy," *Journal of Social Policy*, *44*(4): 747–768.

De Zan, T. (2016a). "Criticità nell'architettura istituzionale a protezione dello spazio cibernetico nazionale," n.117, Approfondimenti, Osservatorio di politica internazionale, www.parlamento.it/application/xmanager/projects/parlamento/file/repository/affariinternazionali/osservatorio/approfondimenti/PI0117App.pdf

De Zan, T. (2016b). "Nuova politica di sicurezza cibernetica per l'Italia," Affarinternazionali, www.affarinternazionali.it/2016/04/nuova-politica-di-sicurezza-cibernetica-per-litalia/

Dentons. (2018, November 21). "European cybersecurity Standards and Their Implementation within the Italian Legislative Framework." dentons.com/en/insights/articles/2018/november/21/european-cybersecurity-standards-and-their-implementation-within-the-italian-legislative-framework

Fritzon, A., Ljungkvist, K., Boin, A., & Rhinard, M. (2007). "Protecting Europe's Critical Infrastructures: Problems and Prospects," *Journal of Contingencies and Crisis Management*, *15*(1): 30–41.

Giacomello, G. (2005). *National Governments and the Control of the Internet: A Digital Challenge*. London and New York: Routledge.

Giacomello, G. (2018). "Va Pensiero: The Evolution of Italy's Information Society," in M. Evangelista (ed.), *Italy From Crisis To Crisis: Political Economy, Security and Society in the 21st Century* (pp. 199–218). London and New York: Routledge.

Horowitz, J. (2018, March). "Will Russia Meddle in Italy's Election? It May Not Have To," *The New York Times*: A8. www.nytimes.com/2018/03/01/world/europe/italy-election-russia.html

Martino, L. (2018a). *Cyber Space and International Relations: Diplomatic Initiatives to Improve Cooperation and Mitigate the Risk of Military Escalation*. Toronto: Thomson Reuters.

Martino, L. (2018b). "National Regulatory Scenario: DPCM Gentiloni and the National Plan for Cyber Protection and IT Security," in R. Baldoni, R. De Nicola, & P. Prinetto (eds.), *The Future of cybersecurity in Italy: Strategic Design Areas* (pp. 18–24). Rome, Italy: Consorzio CINI.

Martino, L. (2018c). *Give Diplomacy a Chance: Give Diplomacy a Chance: OSCE's Red Lines in Cyberspace*. Milan, Italy: Istituto per gli Studi di Politica Internazionale. www.ispionline.it/it/pubblicazione/give-diplomacy-chance-osces-red-lines-cyberspace-20377

Ministry of Foreign Affairs. (2017, April 22). “G7 Declaration on Responsible States Behavior in Cyberspace.” www.mofa.go.jp/files/000246367.pdf

OSCE Permanent Council. (2012, April 26). “Decision No. 1039: Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies,” OSCE document PC.DEC/1039. www.osce.org/pc/90169

OSCE Permanent Council. (2013, December 3). “Decision No. 1106: Initial set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.” www.osce.org/pc/109168?download=true

OSCE Permanent Council. (2016, March 10). “Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.” www.osce.org/pc/227281?download=true

Perrow, C. (2011 [1984]). *Normal Accidents: Living with High Risk Technologies*. Princeton: Princeton University Press.

Presidency of the Council of Ministers. (2017). “National Plan for Cyber Protection and IT Security.” www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

Presidenza del Consiglio dei ministri. (2017). “Piano nazionale per la protezione cibernetica e la sicurezza informatica.” www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

Siroli, G., Giacomelli, R., & Capiluppi, P. (1997). “Internet e World Wide Web,” in P. Capiluppi (ed.), *Reti Informatiche* (pp. 43–51). Le Scienze Quaderni No. 95. Milan: Le Scienze.

Sistema di informazione per la sicurezza della Repubblica. (2017). “Relazione sulla politica dell’informazione per la sicurezza 2016,” Presidenza del Consiglio dei Ministri, Rome, Italy. www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/02/relazione-2016.pdf

Sistema di informazione per la sicurezza della Repubblica. (2018). *Relazione sulla politica dell’informazione per la sicurezza 2017*. Rome, Italy: Presidenza del Consiglio dei Ministri. www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/02/Relazione-2017.pdf

Taormina Leader’s Communiqué. (2017, May 27). www.g7.utoronto.ca/summit/2017taormina/G7-Taormina-Leaders-Communique.pdf

Vestito, F. (2018). *The Italian Cyber Defence Build-Up*. Milan, Italy: Istituto per gli studi di politica internazionale. www.ispionline.it/sites/default/files/pubblicazioni/commentary_vestito_02.05.2018.pdf